INTERNET / E-MAIL POLICY

Version	Date of Issue	Summary of Change	Author
2		Revised	Paula Pocock

1. BACKGROUND

Merseyside Waste Disposal Authority (the Authority) provides many and diverse Information and Communication Technology (ICT) Services, tools and equipment to employees (users) to be used in the course of their work, including computers, laptops, telephones, internet and E-mail.

The Internet has become an essential tool which the Authority uses to comply with statutory obligations as well as general communication, research and educational purposes. Internally, the Authority has also developed an Intranet site to aid the dissemination of relevant information amongst employees.

The Authority supports information and communications resources which will enhance the business and service environment. However, with access to computers and people all over the world via Information and Communications Technology (ICT) comes the availability of material that may not be considered of value in the context of the Authority setting. Additionally, as with any resource, there is the possibility of misuse. Accordingly, the Authority needs to set guidelines for the use of ICT and, where appropriate, to monitor its use.

However, even with guidelines, the Authority cannot prevent the possibility that some users may access material, even inadvertently, that is not consistent with this or other policies of the Authority or in line with the normal duties and responsibilities of the staff member.

2. OBJECTIVES

This policy sets out the rules by which the Authority expects users to employ the ICT services and equipment in order to carry out their duties in a sensible, professional and lawful manner and in accordance with the Authority's Code of Conduct for Officers.

The guidelines aim to set out the Authority's policy on the use and monitoring of ICT and seeks to strike a balance between users' rights to privacy and the Authority's responsibility to ensure appropriate use of ICT.

Failure to comply with these guidelines may be viewed as a disciplinary matter and may therefore, be subject to the Authority's agreed Disciplinary Procedure.

All Officers should read this document carefully before signing the Agreement Form (Appendix A).

3. REVIEW OF GUIDELINES

It is intended that from time to time, as is required by changes to legislation, technology or Authority policy, these Guidelines will be reviewed. Any changes made will be communicated to all users.

4. GENERAL GUIDELINES ON INFORMATION

All information, whether electronic or paper based, relating to our customers, suppliers and business operations should be treated in line with (a) the Authority's Code of Conduct for (b) relevant legislation, and in particular:

Legislation:

Copyright, Designs and Patents Act 1988 – downloading, copying, processing or distributing information from the Internet may be an infringement of copyright or other intellectual property rights.

Data Protection Act 1998 – care should be taken in the collection, processing or disclosure of any personal data and all personal data should be processed within the principles of the Act.

Freedom of Information Act 2000 – all recorded information is potentially disclosable under the Act, including all expressions of fact, intent and opinion. If a request for information is made, the Act prohibits destruction of the information until it is given out in response to the request.

E-mail Disclaimer:

All external e-mail's will automatically carry the following disclaimer;

'This email and any file transmitted with are confidential, subject to copyright and intended solely for the use of the individual or entity to whom they are addressed. It may contain privileged information. Any unauthorised review, use, disclosure, distribution or publication is prohibited. Any views or opinions expressed in this e-mail are those of the author and do not necessarily represent those of the Authority.

If you have received this e-mail in error please contact the sender by reply e-mail and destroy and delete the message and all copies from your computer.

This message has been scanned for viruses, however Merseyside Waste Disposal Authority accept no responsibility for any loss or damage resulting from use of this e-mail. '

5. PERSONAL USE

Any reasonable personal use of the Authority's ICT services and equipment must comply with the Authority's Codes of Conduct for Officers.

Reasonable personal use of such services and equipment:

- Should not interfere with the performance of your duties.
- Should not take priority over your work responsibilities.
- Should not result in the Authority incurring expense.
- Should not have a negative impact on the Authority.
- Should be lawful and in accordance with the Authority Policy and the Guidelines as set out in this document.

Where reasonable personal use is referred to in this document, this section applies.

6. USE OF THE INTERNET

6.1 General Guidelines on use of the Internet.

Use of the Internet is available at your line manager's discretion.

In general, users shall only use the Internet for official purposes. Use of information from the Internet shall be directly related to the official duties of the user, or the Authority as a whole. All information downloaded from the Internet shall be related to the duties and tasks of the user. However, reasonable personal use is permitted in the users own time.
Access to the Internet from the Authority desktop PC must only be undertaken via the Authority's own Internet server.

Users must be aware that the quality and accuracy of information available on the Internet is variable. It is the responsibility of the individual user to judge whether the information obtained is satisfactory for the purpose for which it will be used, and, if appropriate, steps should be taken to verify this information independently.

Where the Internet is being accessed by employees via a laptop or Personal Digital Assistant (PDA) from an internet connection which is not covered by the Authority's internet filtering software, the same guidelines

on appropriate use of the Internet apply and extra care must be taken not to visit sites which would be deemed unsuitable.

No personally owned ICT equipment may be attached to the Authority's network.

6.2 Specific Guidelines on use of the Internet

There must be no interaction (e.g. shopping, entering competitions, gambling, use of credit cards, financial services etc.) The Authority will not be held responsible for any fraudulent actions.

Orders for goods purchased for Authority purposes must not be placed by way of the Internet without the employee having first obtained approval from their line manager any orders placed this way must first be authorised through the Authority's Procurement System and having complied with the Authority's Contract Procedural Rules.

Users must not use their access to the Internet for their own private business purposes.

Users must not intentionally access or transmit information which is obscene, sexually explicit, racist or defamatory or which depicts violent or criminal acts or otherwise represents values that are contrary to Authority policy

The downloading of entertainment software, games, music or screen savers or the playing of games against an opponent via the Internet is forbidden.

Users must not use the Authority Internet facility for the purpose of gambling.

Users should ensure that any material received via external bodies which contains material of an explicit nature should not be forwarded.
Users must not copy information originating from others and re-post it without permission or acknowledgement to the original source.

Users must not break or attempt to break any system security controls placed on their Internet Account.

Users must not intentionally access or transmit computer viruses or software programs used to trigger these

Software, including MP3 files, must not be downloaded from the Internet by users without the advice of the Corporate Services Manager.

Any software or files downloaded via the Internet becomes the property of the Authority.

When participating in newsgroups or mailing lists, users may offer information and advice to others if it is appropriate to their official duties or tasks or if the benefit to be gained by the Authority represents a reasonable return in terms of effort involved.

Employees must not take part in discussions on political matters via the Internet unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited Trade Union Representative.

If an Internet site containing unsuitable material e.g. of an obscene nature is inadvertently accessed by a user, this must be reported immediately to their line manager.

Users must not intentionally access or transmit information of a political nature unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited Trade Union Representative.

Users must not knowingly do anything that constitutes breaking the law.

Access to the Internet and e-mail is controlled by your network login. You should not allow others to use your login to access these facilities. The officer whose user ID and password are utilised will be held responsible. Internet logs are maintained and inspected which record such details as sites accessed and user details. If you have any concerns regarding the security of your login, you should contact the Corporate Services Manager.

6.3 Monitoring and Reporting of Internet Use

All access to the Internet is automatically logged against an address unique to the PC of the user and may be monitored by the Authority. This monitoring will be for the prevention and detection of unauthorised use of the Internet.

Internet filtering software is used to block access to sites which have been deemed unacceptable. In certain cases, where authorised by a line manager, staff in specific posts may be allowed to access sites normally

blocked to users where access to sites is requires or helpful in the undertaking of the duties of the post.

7. USE OF E-MAIL

7.1 General Guidelines on use of E-Mail

The Authority relies on E-mail as an important and significant channel of communication both within the Authority and to communicate with external contacts.

The following guidelines outline the Authority's Policy and the responsibilities of users in the use of the e-mail system provided by the Authority.

E-mail is provided for official purposes. However, it is recognised that staff may wish to use email for personal reasons, but this should be the exception. Personal e-mails should be marked "Personal" in the subject heading.

When using e-mail as a means of communication, it should be kept in mind that:

- E-mails are potentially subject to disclosure under the Freedom of Information Act 2000, including all expressions of fact, intent and opinion.
- E-mails may also be produced in court in the same manner as any other document.
- E-mail communications, either internally or via the internet, are neither guaranteed to be private nor to arrive at their destination either on time or at all.
- Advice given by e-mail has the same legal effect as that given in any written format.
- All e-mail will have the Authority's agreed disclaimer attached.

7.2 Specific Guidelines for the use of E-mail

All e-mail communications must be dealt with in the same manner as a letter, memo or other business communication.

Users must not transmit confidential, sensitive or personal information via e-mail as this may constitute a breach of security under the terms of the Data Protection Act 1998.

Guidelines applying to use of the e-mail system also apply to personal e-mails.

Users must not take part in discussions on political matters via either the Internet or e-mail unless this forms part of the legitimate business of their employment or is in furtherance of their role as an accredited Trade Union Representative.

E-mail may not be used by users to run a business.

Users must not send abusive, insulting, harassing, discriminatory or obscene e-mail messages and/or attachments.

Users must not use e-mail for the purposes of gambling.

Users must not use e-mail to abuse others.

Users must not participate in the sending of chain or pyramid letters.

Users must not forward material which has been emailed to them directly without the permission of the originator, unless the information is forwarded for reasons of normal Authority business.

Where the content of an attachment sent by e-mail requires to exist in its original format only, all reasonable steps must be taken by the sender to ensure the document cannot be changed e.g. use of password protection. This will be dependant on the software used to create the document.

Users must always use their own unique e-mail address when sending e-mails, even when answering e-mails sent to another user.

Users must not falsify e-mails to appear as if sent from someone else or to provide false information to any Internet service requiring an e-mail address or other details.

Users should avoid sending large e-mail attachments greater than 2 megabytes (MB).

Users should not open electronic attachments if the source of such an attachment is unclear without checking with the Information Officer

Users should retain messages which are necessary for current Authority business needs in their mailbox. All unnecessary mail documents – obsolete message, return receipts and attachments should be deleted from the system.

Users must not read, delete, copy or modify the contents of the mailbox of another employee or member without the proper authority, which is generally the authorisation of the line manager of the employee whose mailbox is being accessed.

If an email containing unsuitable material e.g. of an obscene nature is received by a user, this must be reported immediately to their line manager.

7.3 MONITORING AND REPORTING E-MAIL USE

Monitoring is carried out automatically to block inappropriate or malicious sent and received emails.

In general, the Authority respects the users' privacy and autonomy in electronic communications. However, the Authority reserves the right to access, record or monitor the contents of emails both sent and received via the Authority mail system, in order to:

- Provide evidence of business transactions
- Ensure that the Authority business and security procedures are adhered to
- Access communications where necessary in the event of a user's absence from the office
- Access communications to and from an ex-user.

In the case of an investigation required to be carried out into the use of e-mail by a user, the Corporate Services Manager will access the necessary monitored information and provide a report of this to the relevant Manager.

E-mails marked as 'Personal' will generally be excluded from investigation unless there is good reason to suspect that abuse has occurred through the use of personal e-mail.

8 LAPTOPS AND MOBILE STORAGE EQUIPMENT

Increasingly, laptops and other forms of mobile electronic storage equipment – PDAs, USB storage devices etc – are being used to help conduct the business of the Authority. Users of such equipment must ensure that these devices are stored securely and used legally in accordance with these Guidelines.

All devices kept within Authority Premises should be stored securely, and away from windows wherever practicable when not in use. Data held on such devices should be password protected wherever possible.

All users of such equipment are responsible for the security of the equipment itself and for the data which is stored on it. Protecting the equipment and the data from viruses forms an essential part of that responsibility.

When mobile equipment is used out of the office environment the following applies:

• It should be stored as securely as possible and out of view e.g. locked in a carboot or stored in a locked house.

• It should not be left unattended in public.

• Laptops should have up-to-date virus protection software installed. It is the responsibility of the user to ensure that this software is kept up to date.

• Equipment should not be connected to a network other than that of the Authority without the permission of the line manager and guidance of the Corporate Services Manager.

• Files from mobile devices should only be transferred to a computer on the Authority network where the computer has virus protection software installed.

• Equipment should not be used for personal use without the consent of the line manager.

• Extreme caution should be taken when files containing personal or sensitive information are carried on such equipment. Wherever possible, such files should be password protected. Care should be taken that such personal information cannot be seen in a public place by a third party or accessed by unauthorised persons.

• Where such equipment is used out of the office environment, it is the responsibility of the user to ensure that all Health and Safety considerations for the operation of such equipment are taken into account, including Display Screen Equipment Regulations, trip hazards etc.

• Any loss of, damage to or unauthorised access of such equipment or data must be reported as soon as reasonably practicable to your line manager. Any stolen property should be notified immediately to the Corporate Services Manager.

9. TELECOMMUNICATIONS EQUIPMENT

9.1 Use of telecommunications equipment

The Authority provides telephones and mobile telephones to users to carry out the business of the Authority. In general, limited personal use of both is allowed where it has been authorised by the line manager.

All communications carried out by means of telephone should be conducted in a professional manner and not breach the Code of Conduct of Employees.

Calls or texts should not be made to conduct a business other than that of the Authority.

If a call, text or email message is received containing unsuitable material that would constitute a breach of Authority Policy or is offensive to the individual, it must not be forwarded or replied to. The individual may then, should they wish to take the matter further, report this immediately to their line manager who may determine what action will be taken in relation to the sender.

All mobile telephones should be kept securely and appropriate security measures should be taken to ensure that they, or data held on them, are not subject to loss, damage or unauthorised access.

Any loss or damage to telephone equipment should be notified to the line manager as soon as reasonably practicable.

Mobile phones should be used in accordance with the guidelines issued by the Authority and in particular should not be used

- whilst driving.
- in places where such use is prohibited or restricted.

9.2 MONITORING

Details of all calls made by both land lines and mobile phones are recorded including the date, time and duration of the call on an itemised bill from the service provider.

10. HOME WORKING/REMOTE WORKING

When using Authority systems or equipment (such as laptops) or using your own computer equipment to work on Authority business away from the Authority's premises, the following rules apply:

• All work related to the business of the Authority must be password protected.

• All work, in particular where personal or sensitive information is involved, should be carried out in a position where it cannot be seen by others.

• All reasonable precautions should be taken to safeguard the security of any Authority equipment or data regardless of the medium it is stored in – paper, diskette, CD, USB device or laptop.

• In accordance with principle seven of the Data Protection Act 1998, appropriate measures must be taken to ensure the security of personal data which comes into your possession in the course of your employment to prevent it from theft, loss, destruction or harm either accidental or malicious.

• Any files saved remotely should be transferred to the Authority's System as soon as is practicable.

• Health and Safety consideration around the use of such equipment remotely or at home is the responsibility of the employee.

11. MISUSE

It is the responsibility of every user to use these services and equipment appropriately, legally and in accordance with these Guidelines and the wider policies of the Authority including the Code of Conduct for Officers.

Furthermore, it is a criminal offence under the Computer Misuse Act 1990 to carry out the following activities:

• Unauthorised access to computer material i.e. hacking

• Unauthorised modification of computer material

• Unauthorised access to computer material with the intent to commit or facilitate the commission of further offences.

• Undertake the harassment of others by electronic means.

The Authority reserves the right to withdraw Internet access or E-mail use – or any access to the Authority's computer or communications network – if the user has been found to be in breach of these guidelines.

The Authority reserves the right to prohibit access to specific newsgroups or Internet sites or other Internet resources or to remove or substitute the hardware or software used to access the Internet at any time for any reason.

Any breach of these guidelines will be viewed seriously and may result in action being taken under the Authority's Disciplinary Procedures. Additionally, the Authority is legally obliged to co-operate with the Police, Inland Revenue and Customs and Excise in the investigation and detection of crime and apprehension of offenders. This may involve allowing such bodies' access to the monitoring records of or equipment held by an individual employee.

Appendix A

Agreement Form

I have read and understand Merseyside Waste Disposal Authority Internet and E-Mail Policy and agree to comply with these guidelines.

I understand that any deliberate breach of these will be viewed seriously and may result in action being taken under the Authority's disciplinary procedures which may include the withdrawal of access to either E-mail or Internet facilities or both.

I accept that all access to the Internet is recorded and may be monitored and that any 'irregularities' encountered in this process will be reported to my line manager.

I agree that if I inadvertently access any Internet site containing unsuitable material, or receive an email with inappropriate content I will report this matter to my line manager.

Signed ……..

Section …….

Date ……..

(Please complete and return to the Assistant Corporate Services Manager)